

August 28, 2014

# MOR CRYPTOSYSTEM AND CLASSICAL CHEVALLEY GROUPS IN ODD CHARACTERISTIC

AYAN MAHALANOBIS AND ANUPAM SINGH

*IISER Pune, Dr. Homi Bhabha Road, Pashan, Pune 411008, INDIA.*

**ABSTRACT.** In this paper we study the MOR cryptosystem with finite Chevalley groups. There are four infinite families of finite classical Chevalley groups. These are: special linear groups  $SL(d, q)$ , orthogonal groups  $O(d, q)$  and symplectic groups  $Sp(d, q)$ . The family  $O(d, q)$  splits to two different families of Chevalley groups depending on the parity of  $d$ . The MOR cryptosystem over  $SL(d, q)$  was studied by the first author, “A simple generalization of the ElGamal cryptosystem to non-abelian groups II, Communications in Algebra 40 (2012), no. 9, 3583–3596”. In that case, the hardness of the MOR cryptosystem was found to be equivalent to the discrete logarithm problem in  $\mathbb{F}_{q^d}$ . In this paper, we show that the MOR cryptosystem over  $Sp(d, q)$  has the security of the discrete logarithm problem in  $\mathbb{F}_{q^d}$ . However, it seems likely that the security of the MOR cryptosystem for the family of orthogonal groups is  $\mathbb{F}_{q^{d^2}}$ . We also develop an analog of row-column operations in orthogonal and symplectic groups.

## 1. INTRODUCTION

Public-key cryptography is a backbone of this modern society. However with **recent advances in the index-calculus algorithm to solve the discrete logarithm problem in finite fields of small characteristic** by Joux [2, 14], and its possible implication to factoring algorithms, it seems that we are left with only one cryptographic primitive – the discrete logarithm problem in the group of rational points of an elliptic curve over a finite field. So it seems prudent that we set out in search for new cryptographic primitives and subsequently new cryptosystems. The obvious question is: how to search and where to look? One can look into several well-known hard problems in Mathematics and hope to create a trap-door function or one can try to generalize the known, trusted cryptosystems.

This paper is in the direction of generalizing a known cryptosystem with the hope that something practical and useful will come out of this generalization. A new but arbitrary cryptosystem might not be considered by the community as a secure cryptosystem for decades. So our approach is conservative but practical.

The cryptosystem that we have in mind is *the MOR cryptosystem* [17–19]. It is a simple but powerful generalization of the well known and classic ElGamal cryptosystem. In this cryptosystem the discrete logarithm problem works in the automorphism group of a group instead of the group. As a matter of fact, it can work in the automorphism group of most algebraic structures. However, we will limit ourselves to finite groups. One way

---

*E-mail address:* ayan.mahalanobis@gmail.com, anupamk18@gmail.com.

2010 *Mathematics Subject Classification.* 94A60, 20H30.

*Key words and phrases.* MOR cryptosystem, Chevalley groups, public-key cryptography.

This work was supported by a SERB research grant.

to look at the MOR cryptosystem is that it generalizes the discrete logarithm problem from a cyclic (sub)group to an arbitrary group.

The MOR cryptosystem over  $\text{SL}(d, q)$  was studied earlier [17] and the work for finite  $p$ -groups is due to appear [18]. It became clear that working with matrix groups of size  $d$  over  $\mathbb{F}_q$  and with automorphisms that act by conjugation, like the inner automorphism, there are two possible reductions of the security to finite fields. It is the security of the discrete logarithm problem in  $\mathbb{F}_{q^d}$  or  $\mathbb{F}_{q^{d^2}}$  [17, Section 7]. This reduction is similar to the embedding of the discrete logarithm problem in the group of rational points of an elliptic curve to a finite field, the degree of the extension of that field over the field of definition of the elliptic curve is called the *embedding degree*. In the case of  $\text{SL}(d, q)$ , it became the security of  $\mathbb{F}_{q^d}$ . The reason that we undertook this study, is to see, if the security in other classical Chevalley groups is  $\mathbb{F}_{q^d}$  or  $\mathbb{F}_{q^{d^2}}$ .

Though in cryptography it is often hard to come up with theorems about security of a cryptosystem, we were able to show that the attack that embeds the security of  $\text{SL}(d, q)$  to a discrete logarithm problem in  $\mathbb{F}_{q^d}$  works for symplectic groups as well. However, at this moment it seems likely that the security of the MOR cryptosystem in orthogonal groups  $\text{O}(d, q)$  is  $\mathbb{F}_{q^{d^2}}$ . The way we implement this cryptosystem is by solving the word problem in generators. It presents no advantage to small characteristic. In the light of Joux's [2] improvement of the index-calculus attack in small characteristic, this contribution of the MOR cryptosystem is remarkable.

**In summary**, the proposed MOR cryptosystem is totally different from the known ElGamal cryptosystems from a functional point of view. Its implementation depends on row-column operations and substitutions (substituting a matrix for a word in generators). However, we do have a concrete and tangible understanding of its security.

**1.1. Finite groups that we consider in this paper.** In this paper, we work with finite fields of odd characteristic. We work with classical Chevalley groups  $\text{O}(2l+1, q)$ ,  $\text{Sp}(2l, q)$  and  $\text{O}(2l, q)$  of  $B_l$ ,  $C_l$  and  $D_l$  type respectively for  $l \geq 2$ . Note that the group  $\text{SL}(l+1, q)$  of  $A_l$  type has been dealt with earlier [17]. Our analysis and the subsequent conclusions hold for central (and subgroups of the center) quotients of the above mentioned groups and with any proper characteristic subgroups, like the commutator of the above groups. In this paper, we do not consider *twisted classical Chevalley groups*, also called Steinberg groups. These are the  ${}^2A_l(q)$  type which is the unitary group  $\text{U}(l+1, q)$  and  ${}^2D_l(q)$  type which is the orthogonal group  $\text{O}^-(2l, q)$  [5, Section 14.5]. We hope to continue our study with these groups in subsequent publications.

**1.2. Structure of the paper.** This paper is a study of the MOR cryptosystem using the orthogonal and symplectic groups over finite fields of odd characteristic.

In Section 2, we describe the MOR cryptosystem in some details. We emphasize that the MOR cryptosystem is a natural generalization of the classic ElGamal cryptosystem. In Section 3, we describe the orthogonal and symplectic groups and their automorphisms. In Section 6, we describe two new algorithms. These algorithms use the row-column operations to write an element in the orthogonal or symplectic group as a word in generators. This is very similar to the row-column operations in special linear groups. These algorithms are useful in the implementation of the MOR cryptosystem. These algorithms are also of independent interest in computational group theory. We conclude this paper with some implementation details.

**1.3. Notations and terminology.** It was bit hard for us to pick notations for this paper. The notations used by a Lie group theorist is somewhat different from that of a computational group theorist. We tried to preserve the essence of notations as much as possible. For example, a Lie group theorist will use  $SL_{l+1}(q)$  to denote what we will denote by  $SL(l+1, q)$  or  $SL(d, q)$ . We have used  ${}^T X$  to denote the transpose of the matrix  $X$ . This was necessary to avoid any confusion that might arise when using  $X^{-1}$  and  ${}^T X$  simultaneously. In this paper, we use  $K$  and  $\mathbb{F}_q$  interchangeably, while each of them is a finite field of odd characteristic. All other notations used are standard.

## 2. THE MOR CRYPTOSYSTEM

The MOR cryptosystem is a natural generalization of the classic ElGamal cryptosystem. It was first proposed by Paeng et. al. [19]. To elaborate the idea behind a MOR cryptosystem we take a slightly expository route. For the purpose of this exposition, we define **the discrete logarithm problem**. It is one of the most common cryptographic primitive in use. It works in any cyclic (sub)group  $G = \langle g \rangle$ , but is not secure in any cyclic group.

**Definition 2.1** (The discrete logarithm problem). *The discrete logarithm problem in  $G = \langle g \rangle$  is, given  $g$  and  $g^m$  find  $m$ .*

The word “find” in the above definition is bit vague, in this paper we mean compute  $m$ . The hardness to solve the discrete logarithm problem depends on the presentation of the group and is not an invariant under isomorphism. It is believed that the discrete logarithm problem is secure in the multiplicative group of a finite field and the group of rational points of an elliptic curve. The security in elliptic curves is considered much better than that of finite fields because of non-existence of sub-exponential algorithms in most cases of elliptic curves [1, 21].

A more important cryptographic primitive, related to the discrete logarithm problem is the **Diffie-Hellman problem**, also known as the **computational Diffie-Hellman problem**.

**Definition 2.2** (Diffie-Hellman problem). *Given  $g$ ,  $g^{m_1}$  and  $g^{m_2}$  find  $g^{m_1 m_2}$ .*

It is clear, if one solves the discrete logarithm problem then the Diffie-Hellman problem is solved as well. The other direction is not known.

The most prolific cryptosystem in use today is the ElGamal cryptosystem. It uses the cyclic group  $G = \langle g \rangle$ . It is defined as follows:

### 2.1. The ElGamal cryptosystem.

A cyclic group  $G = \langle g \rangle$  is public.

- **Public-key:** Let  $g$  and  $g^m$  is public.
- **Private-key:** The integer  $m$  is private.

#### Encryption:

To encrypt a plaintext  $\mathfrak{M} \in G$ , get an arbitrary integer  $r \in [1, |G|]$  compute  $g^r$  and  $g^{rm}$ . The ciphertext is  $(g^r, \mathfrak{M}g^{rm})$ .

#### Decryption:

After receiving the ciphertext  $(g^r, \mathfrak{M}g^{rm})$ , the user uses the private key  $m$ . So she computes  $g^{mr}$  from  $g^r$  and then computes  $\mathfrak{M}$ .

It is well known that the hardness of the ElGamal cryptosystem is equivalent to the Diffie-Hellman problem [13, Proposition 2.10].

**2.2. The MOR cryptosystem.** In the case of the MOR cryptosystem, one works with the automorphism group of a group. An automorphism group can be defined on any algebraic structure and subsequently a MOR cryptosystem can also be defined on that automorphism group, however in this paper we restrict ourselves to finite groups. Furthermore, we look at *classical groups* defined by generators and automorphisms are defined as actions on those generators.

Let  $G = \langle g_1, g_2, \dots, g_s \rangle$  be a finite group. Let  $\phi$  be a non-identity automorphism.

- **Public-key:** Let  $\{\phi(g_i)\}_{i=1}^s$  and  $\{\phi^m(g_i)\}_{i=1}^s$  is public.
- **Private-key:** The integer  $m$  is private.

**Encryption:**

To encrypt a plaintext  $\mathfrak{M} \in G$ , get an arbitrary integer  $r \in [1, |\phi|]$  compute  $\phi^r$  and  $\phi^{rm}$ . The ciphertext is  $(\phi^r, \phi^{rm}(\mathfrak{M}))$ .

**Decryption:**

After receiving the ciphertext  $(\phi^r, \phi^{rm}(\mathfrak{M}))$ , the user knows the private key  $m$ . So she computes  $\phi^{mr}$  from  $\phi^r$  and then computes  $\mathfrak{M}$ .

**Theorem 2.1.** *The hardness to break the above MOR cryptosystem is equivalent to the Diffie-Hellman problem in the group  $\langle \phi \rangle$ .*

*Proof.* It is easy to see that if one can break the Diffie-Hellman problem then one can compute  $\phi^{mr}$  from  $\phi^m$  in the public-key and  $\phi^r$  in the ciphertext. This breaks the system.

On the other hand, observe that the plaintext is  $\phi^{-mr}(\phi^{mr}(\mathfrak{M}))$ . Assume that there is an oracle that can break the MOR cryptosystem, i.e., given  $\phi, \phi^m$  and a plaintext  $(\phi^r, g)$  will deliver  $\phi^{-mr}(g)$ . Now we query the oracle  $s$  times with the public-key and the ciphertext  $(\phi^r, g_i)$  for  $i = 1, 2, \dots, s$ . From the output one can easily find  $\phi^{mr}(g_i)$  for  $i = 1, 2, \dots, s$ . So we just witnessed that for  $\phi^m$  and  $\phi^r$  one can compute  $\phi^{mr}$  using the oracle. This solves the Diffie-Hellman problem. •

In a practical implementation of a MOR cryptosystem there are two things that matter the most.

- a:** The number of generators. As we saw that the automorphism  $\phi$  is presented as action on generators. Larger the number of generators bigger is the public-key.
- b:** Efficient algorithm to solve the word problem. This means, given  $G = \langle g_1, g_2, \dots, g_s \rangle$  and  $g \in G$ , is there an efficient algorithm to write  $g$  as word in  $g_1, g_2, \dots, g_s$ ? The reason of this importance is immediate – the automorphisms are presented as action on generators and if one has to compute  $\phi(g)$ , then the word problem must be solved.

The obvious question is: what are the right groups for the MOR cryptosystem? In this paper, we pursue a study of the MOR cryptosystem using **finite Chevalley groups** of classical type, in particular, orthogonal and symplectic groups.

### 3. CLASSICAL GROUPS

In this section, we produce a brief overview of the Chevalley groups of classical type. We introduce orthogonal and symplectic groups. References for this section are Carter [5] and Grove [9]. We also briefly describe similitude groups which are required for a study of diagonal automorphisms of the Chevalley groups. In this section we fix notation which will be used throughout this paper.

Let  $V$  be a vector space of dimension  $d$  over a field  $K$  of odd characteristic. Let  $\beta: V \times V \rightarrow K$  be a bilinear form. By fixing a basis of  $V$  we can associate a matrix to  $\beta$ . We shall abuse the notation slightly and denote the matrix of the bilinear form by  $\beta$  itself. Thus  $\beta(x, y) = {}^t x \beta y$  where  $x, y$  are column vectors. We will work with non-degenerate bilinear forms and that means  $\det \beta \neq 0$ . A symmetric or skew-symmetric bilinear form  $\beta$  satisfies  $\beta = {}^t \beta$  or  $\beta = -{}^t \beta$  respectively.

**Definition 3.1** (Orthogonal Groups). *A square matrix  $X$  of size  $d$  is called orthogonal if  ${}^t X \beta X = \beta$  where  $\beta$  is symmetric. It is well known that the orthogonal matrices form a group known as the orthogonal group.*

**Definition 3.2** (Symplectic Group). *A square matrix of size  $d$  is called symplectic if  ${}^t X \beta X = \beta$  where  $\beta$  is skew-symmetric. And the set of symplectic matrices form symplectic group.*

We write the dimension of  $V$  as  $d = 2l + 1$  or  $d = 2l$  for  $l \geq 1$ . We fix a basis and index it by  $0, 1, 2, \dots, l, -1, -2, \dots, -l$  for odd dimension and by  $1, 2, \dots, l, -1, -2, \dots, -l$  for even dimension. We consider the non-degenerate bilinear forms  $\beta$  on  $V$  given by the following matrices:

- Type  $B_l$ : The form  $\beta$  is symmetric with  $d = 2l + 1$  and  $\beta = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix}$ .
- Type  $C_l$ : The form  $\beta$  is skew-symmetric with  $d = 2l$  and  $\beta = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$ .
- Type  $D_l$ : The form  $\beta$  is symmetric with  $d = 2l$  and  $\beta = \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix}$ .

where  $I_l$  is the identity matrix of size  $l$  over  $K$ .

Let  $K (= \mathbb{F}_q)$  be a finite field of odd characteristic. If  $d$  is odd there is only one orthogonal group up to conjugation [9, Page 79] and thus we can fix  $\beta$  as above of  $B_l$  type. In this case the orthogonal group is simply denoted by  $O(2l + 1, q)$ . Up to equivalence there is only one non-degenerate skew-symmetric form in even dimension [9, Theorem 2.10]. We fix  $\beta$  of  $C_l$  type as above. Thus there is only one symplectic group up to conjugation denoted by  $Sp(2l, q)$ . However up to conjugation there are two different orthogonal groups [9, Page 79] in even dimension  $d = 2l$ . In this paper, we work with only one of them corresponding to the  $\beta$  fixed as above of type  $D_l$ . We denote this orthogonal group by  $O(2l, q)$ . The other orthogonal group often denoted as  $O^-(2l, q)$  is twisted Chevalley group denoted as  ${}^2D_l(q)$ , also called Steinberg groups.

**Definition 3.3** (Orthogonal similitude groups). *The orthogonal similitude group is defined as the set of matrices  $X$  of size  $d$  as follows:  $GO(d, q) = \{X \in GL(d, q) \mid {}^t X \beta X = \mu \beta, \mu \in \mathbb{F}_q^\times\}$  where  $d = 2l + 1$  or  $2l$  and  $\beta$  is of type  $B_l$  and  $D_l$  respectively.*

**Definition 3.4** (Symplectic similitude group). *The symplectic similitude group is denoted by  $GSp(2l, q) = \{X \in GL(2l, K) \mid {}^t X \beta X = \mu \beta, \mu \in \mathbb{F}_q^\times\}$  where  $\beta$  is of type  $C_l$ .*

Here  $\mu$  depends on the matrix  $X$  and is called the similitude factor. The similitude factor  $\mu$  defines a group homomorphism from the similitude group to  $\mathbb{F}_q^\times$  and the kernel is the orthogonal group  $O(d, q)$  when  $\beta$  is symmetric and symplectic group  $Sp(2l, q)$  when  $\beta$  is skew-symmetric respectively [15, Section 12]. Note that scalar matrices  $\lambda I$  for  $\lambda \in \mathbb{F}_q^\times$  belong to the center of similitude groups. The similitude groups are thought of analog of

what  $GL(d, q)$  is for  $SL(d, q)$ . For a discussion of the diagonal automorphisms of Chevalley groups we need the diagonal subgroups of the similitude groups.

**Definition 3.5** (Diagonal group). *The diagonal groups are defined to be the group of non-singular diagonal matrices in the corresponding similitude group and are as follows: in the case of  $GO(2l + 1, q)$  it is*

$$\{\text{diag}(\alpha, \lambda_1, \dots, \lambda_l, \mu\lambda_1^{-1}, \dots, \mu\lambda_l^{-1}) \mid \lambda_1, \dots, \lambda_l, \alpha^2 = \mu \in \mathbb{F}_q^\times\}$$

*and in the case of  $GO(2l, q)$  and  $GSp(2l, q)$  it is*

$$\{\text{diag}(\lambda_1, \dots, \lambda_l, \mu\lambda_1^{-1}, \dots, \mu\lambda_l^{-1}) \mid \lambda_1, \dots, \lambda_l, \mu \in \mathbb{F}_q^\times\}.$$

Conjugation by these diagonal elements produce diagonal automorphisms in the respective Chevalley groups.

We denote by  $\Omega_d(q)$  the commutator subgroup of the orthogonal group  $O(d, q)$ . It is a index 2 subgroup of the special orthogonal group  $SO(d, q)$ . We fix a generator of  $SO(d, q)/\Omega_d(q)$  as  $d(\zeta) = \text{diag}(1, 1, \dots, 1, \zeta, 1, \dots, 1, \zeta^{-1})$  where  $\zeta$  is a fixed non-square in  $\mathbb{F}_q$  [9, Theorem 9.7]. Further, the group  $SO(d, q)$  is of index 2 in  $O(d, q)$  and we fix a generator for the quotient as  $w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$  where  $e_{i,j}$  denotes a matrix with 1 at  $(i, j)^{\text{th}}$  place and 0 everywhere else.

**3.1. Chevalley Generators.** To work with Chevalley groups we need a set of generators for these groups. We describe the Chevalley generators from the theory of Chevalley groups [5]. For sake of completeness of this paper, we will briefly go through the theory of Chevalley groups in the next section. In what follows  $t$  varies over  $\mathbb{F}_q$ .

- (1) The group  $SL(l + 1, q)$  is generated by the matrices  $x_{i,j}(t) = I + te_{i,j}$  where  $1 \leq i \neq j \leq l + 1$ . This is Chevalley group of  $A_l$  type.
- (2) For  $1 \leq i, j \leq l$ , the group  $\Omega_{2l+1}(q)$  is generated by the following matrices:

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}), && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) && \text{for } i < j, \\ x_{i,0}(t) &= I + t(2e_{i,0} - e_{0,-i}) - t^2e_{i,-i}, \\ x_{0,i}(t) &= I + t(-2e_{-i,0} + e_{0,i}) - t^2e_{-i,i}. \end{aligned}$$

With these generators the elements  $d(\zeta) = \text{diag}(1, \underbrace{1, \dots, 1}_l, \zeta, \underbrace{1, \dots, 1}_l, \zeta^{-1})$  and

$w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$  generate the orthogonal group  $O(2l + 1, q)$ . This is Chevalley group of  $B_l$  type.

- (3) For  $1 \leq i, j \leq l$ , the group  $Sp(2l, q)$  is generated by the matrices

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} + e_{j,-i}) && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} + e_{-j,i}) && \text{for } i < j, \\ x_{i,-i}(t) &= I + te_{i,-i} \\ x_{-i,i}(t) &= I + te_{-i,i}. \end{aligned}$$

This is Chevalley group of  $C_l$  type.

(4) For  $1 \leq i, j \leq l$ , the group  $\Omega_{2l}(q)$  is generated by the matrices

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) \quad \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}) \quad \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) \quad \text{for } i < j. \end{aligned}$$

With the above generators the elements  $d(\zeta) = \text{diag}(\underbrace{1, \dots, 1}_l, \zeta, \underbrace{1, \dots, 1}_l, \zeta^{-1})$  and

$w_l = I - e_{l,l} - e_{-l,-l} - e_{l,-l} - e_{-l,l}$  generate the orthogonal group  $O(2l, q)$ . This is Chevalley group of  $D_l$  type.

It is interesting to note that our algorithm in Section 6 to solve the word problem in Chevalley groups using the above generators gives yet another proof that the matrices listed above generate the corresponding groups.

#### 4. ADJOINT CHEVALLEY GROUPS

In this section we introduce adjoint Chevalley groups. One could get around without reading this section, we include this to explain why the generators listed in Section 3.1 are natural. The material is not that important to understand the later part of this paper. It is probably impossible to produce a brief and comprehensive introduction to Chevalley groups. The usual route to describe a Chevalley group is as a subgroup of the automorphism group of a *simple Lie algebra*. A Lie algebra over a field is a finite dimensional vector space with a Lie bracket operation. We are particularly interested in simple Lie algebras over  $\mathbb{C}$ . The theory was originally developed by Chevalley [6]. Though our exposition follows Carter [5] and Steinberg [23]. A more general account of this theory over commutative rings can be found in Vavilov [24].

We are particularly interested in simple Lie algebras over  $\mathbb{C}$ . One dimensional Lie algebras are always simple and uninteresting. It is known that a Lie algebra contains a self-normalizing nilpotent subalgebra  $\mathcal{H}$  called the Cartan subalgebra. In case of simple Lie algebras the Cartan subalgebra contains only semi-simple elements. Corresponding to a Cartan subalgebra  $\mathcal{H}$ , we can define a decomposition of the simple Lie algebra  $\mathcal{L}$  by looking at the simultaneous decomposition as eigen-spaces. So we can write  $\mathcal{L} = \mathcal{H} \oplus \bigoplus_{r \in \Phi} \mathcal{L}_r$  where  $\mathcal{L}_r$  are one dimensional subspaces of  $\mathcal{L}$  satisfying  $[h, e_r] = r(h)e_r$  where  $r: \mathcal{H} \rightarrow \mathbb{C}$ ,  $e_r$  is the generator of  $\mathcal{L}_r$  and  $\Phi$  is finite subset of  $\mathcal{H}^*$ , the dual of  $\mathcal{H}$ . This is called a Cartan decomposition of  $\mathcal{L}$  [5, Section 3.2].

The set  $\Phi$  obtained using Cartan decomposition is the root system for the Lie algebra  $\mathcal{L}$ . An abstract root system [5, Definition 2.1.1] is a finite subset of an Euclidean space of the same dimension as  $\mathcal{H}$ . By fixing an order in the Euclidean space we get a system of positive roots  $\Phi^+$  and negative roots  $\Phi^-$  so that  $\Phi = \Phi^+ \cup \Phi^-$ . Let  $\Pi = \{p_1, \dots, p_l\}$  be a system of *simple roots*, i.e., any root is either non-positive or non-negative integer linear combination of simple roots. We denote by  $h_r = 2r/(r, r)$  the co-root corresponding to the root  $r$ , where  $(\cdot, \cdot)$  is the usual inner-product on the Euclidean space containing the roots. It is a theorem of Chevalley that there is a basis  $\{h_r, r \in \Pi; e_r, r \in \Phi\}$  of  $\mathcal{L}$  satisfying the following [5, Theorem 4.2.1]:

$$\begin{aligned} [e_r, e_{-r}] &= h_r, \\ [e_r, e_s] &= 0 \text{ if } r + s \notin \Phi \text{ else } [e_r, e_s] = \pm(p+1)e_{r+s} \text{ where } r \neq \pm s, \\ [h_r, h_s] &= 0, \\ [h_r, e_s] &= A_{rs}e_s, \end{aligned}$$

where  $-pr+s, \dots, -r+s, s, r+s, \dots, qr+s$  is a  $r$ -chain passing through  $s$  and  $A_{rs} = \frac{2(r,s)}{(r,r)}$  are integers known as the *Cartan integers*. Such a basis is called a *Chevalley basis* [5, Section 4.2].

There is a well-known classification of finite dimensional simple Lie algebras over  $\mathbb{C}$  [5, Section 3.6]. They are classified via their Dynkin diagram. There are four infinite families  $A_l(l \geq 1)$ ,  $B_l(l \geq 2)$ ,  $C_l(l \geq 3)$  and  $D_l(l \geq 4)$  together called simple Lie algebras of "classical type" and five "exceptional types"  $G_2, F_4, E_6, E_7$  and  $E_8$ . In Section 4.1 we explicitly describe the classical Lie algebras and their Chevalley basis which will be used to form adjoint Chevalley groups. From now on  $\mathcal{L}$  is one of  $A_l, B_l, C_l$  or  $D_l$ .

Let  $K(=\mathbb{F}_q)$  be a finite field of odd characteristic. We denote by  $\mathcal{L}_{\mathbb{Z}}$  the  $\mathbb{Z}$ -span of a Chevalley basis in  $\mathcal{L}$ . Clearly  $\mathcal{L}_{\mathbb{Z}}$  is a Lie algebra over  $\mathbb{Z}$ . Define  $\mathcal{L}_K = K \otimes \mathcal{L}_{\mathbb{Z}}$ . Then one can define a Lie algebra structure on  $\mathcal{L}_K$  as follows:

$$[1 \otimes x, 1 \otimes y] := 1 \otimes [x, y]$$

for basis elements  $x, y$  and extended by linearity. Thus  $\mathcal{L}_K$  is a Lie algebra over  $K$ .

To define the groups of our interest we need to work with certain operators which are in  $\text{Aut}(\mathcal{L}_K)$ . For this we start by defining  $x_r(\zeta) := \exp(\zeta \text{ad}(e_r)) \in \text{Aut}(\mathcal{L})$  for  $r \in \Phi$  and  $\zeta \in \mathbb{C}$ . Where  $\text{ad}$  is the Lie algebra homomorphism  $\text{ad}: \mathcal{L} \rightarrow \text{End}(\mathcal{L})$  given by  $\text{ad}(x).y = [x, y]$ . These operators  $x_r$  are unipotent operators whose matrix entries are polynomials in  $\zeta$  with integer coefficients. Thus by substituting  $t \in K$  for the variable  $\zeta$  and reducing the coefficients modulo the characteristic of the field  $K$ , we get operators  $x_r(t) \in \text{Aut}(\mathcal{L}_K)$ . The *adjoint Chevalley group of type  $\mathcal{L}$  over  $K$*  is the subgroup of  $\text{Aut}(\mathcal{L}_K)$  generated by  $x_r(t)$  for all  $r \in \Phi$  and  $t \in K$ , and is denoted by

$$\mathcal{L}(K) := \langle x_r(t) \mid r \in \Phi, t \in K \rangle.$$

One can explicitly write down  $x_r(t)$  as an automorphism of  $\mathcal{L}_K$  on the basis elements as follows:

$$\begin{aligned} x_r(t).e_r &= e_r, \\ x_r(t).e_{-r} &= e_{-r} + th_r - t^2 e_r, \\ x_r(t).h_s &= h_s - A_{sr} t e_r \text{ for } s \in \Pi, \\ x_r(t).e_s &= \sum_{i=0}^q M_{r,s,i} t^i e_{i,r+s} \text{ if } r \neq \pm s \end{aligned}$$

where  $M_{r,s,i} = \pm \binom{p+i}{i}$  and  $r, s \in \Phi$ . In this paper we are working with classical Chevalley groups which are explicitly described in Section 4.1.

For a fixed  $r$ , the subgroup  $X_r$  generated by elements  $x_r(t)$  for all  $t \in K$ , is called a root subgroup and is isomorphic to the additive group of  $K$ . Let  $U := \langle X_r \mid r \in \Phi^+ \rangle$  and  $V := \langle X_r \mid r \in \Phi^- \rangle$  be subgroups of  $\mathcal{L}(K)$ . Then both  $U$  and  $V$  are unipotent as well as nilpotent groups. Furthermore these are Sylow  $p$ -subgroups of  $\mathcal{L}(K)$ . For every  $r \in \Phi$  there is a surjective homomorphism [5, Theorem 6.3.1]  $\phi_r: \text{SL}(2, K) \rightarrow \langle X_r, X_{-r} \rangle$  which maps  $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$  to  $x_r(t)$  and  $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$  to  $x_{-r}(t)$ . Let us define  $h_r(\lambda)$  as  $\phi_r \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$  and  $n_r(t)$  as  $\phi_r \begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}$ . Set  $n_r = n_r(1)$  for convenience. We now define some important subgroups  $H := \langle h_r(t) \mid r \in \Phi, t \in K^\times \rangle$  and  $N := \langle H, n_r \mid r \in \Phi \rangle$ .

For our discussion of diagonal automorphisms we need a slightly larger group. Let  $P = \mathbb{Z}\Phi$  be the root lattice and  $Q$  be the weight lattice ( $\mathbb{Z}$  span of the dual of co-roots) [5, Section 7.1]. We know that  $P \subset Q$ . It is known that:



Simple Lie Algebra	$Q/P$
$A_l$	$\mathbb{Z}/(l+1)\mathbb{Z}$
$B_l, C_l$	$\mathbb{Z}/2\mathbb{Z}$
$D_l$	$\mathbb{Z}/4\mathbb{Z}$ if $l$ odd
	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $l$ even

There is a well known isomorphism [5, Section 7.1]  $h: \text{Hom}(P, K^\times) \rightarrow \hat{H} \subset \text{Aut}(\mathcal{L}_K)$  given by  $\chi \mapsto h(\chi)$  where  $h(\chi).h_s = h_s$  and  $h(\chi).e_s = \chi(s)e_s$ . Furthermore  $H \subset \hat{H}$  and  $h(\chi) \in H$  if the character  $\chi$  can be extended to a character of  $Q$ . The group  $\hat{H}$  normalizes  $U$  and  $V$  and hence  $\mathcal{L}(K)$  (refer to the note following [5, Theorem 7.1.1]). Further  $\mathcal{L}(K) \cap \hat{H} = H$ . Let  $\hat{G} \subset \text{Aut}(\mathcal{L}_K)$  be the subgroup generated by  $\mathcal{L}(K)$  and  $\hat{H}$ . Then  $\mathcal{L}(K)$  is a normal subgroup of  $\hat{G}$  and  $\hat{G}/\mathcal{L}(K) \cong \hat{H}/H$ .

We are working with Chevalley groups of classical type which we now describe explicitly.

**4.1. Chevalley Groups of Classical types.** In this section, we describe the Chevalley groups of classical type following Carter [5, Section 11.2 and 11.3]. In each case, we first describe the complex simple Lie algebra. These are subalgebra of the full matrix algebra  $M(d, \mathbb{C})$ , square matrices of size  $d$  over  $\mathbb{C}$ , with bracket operation  $[X, Y] = XY - YX$ . Then we get a Chevalley basis as described earlier and a Lie algebra over  $\mathbb{Z}$  and hence over any field  $K$  by a base change. Using this we describe the root generators  $x_r(t)$  of the adjoint Chevalley group  $\mathcal{L}(K)$ . It turns out that the operators  $x_r(t)$  are inner conjugation automorphism [5, Lemma 4.5.1] on  $\mathcal{L}_K$  by  $\exp(te_r)$  which generate an intermediate Chevalley group denoted as  $\bar{G}$ . The group  $\bar{G}$  is close to groups of our interest. In later section, we will abuse the notation slightly and denote the generators of  $\bar{G}$  as  $x_r(t)$  (for example in the Section 3.1). We make a table before we describe them explicitly.

Type	Group of our interest	$\bar{G}$	$\mathcal{L}(K)$
$A_l$	$\text{SL}(l+1, K)$	$\text{SL}(l+1, K)$	$\text{PSL}(l+1, K)$
$B_l$	$\text{O}(2l+1, K)$	$\Omega_{2l+1}(K)$	$P\Omega_{2l+1}(K)$
$C_l$	$\text{Sp}(2l, K)$	$\text{Sp}(2l, K)$	$\text{PSp}(2l, K)$
$D_l$	$\text{O}(2l, K)$	$\Omega_{2l}(K)$	$P\Omega_{2l}(K)$

**Type  $A_l$  :** The  $A_l$  type complex Lie algebra is  $sl_{l+1}(\mathbb{C})$  consisting of trace 0 matrices of size  $l+1$ . The set of all diagonal matrices in  $sl_{l+1}(\mathbb{C})$  give a Cartan subalgebra and that Cartan decomposition gives a Chevalley basis. The roots (eigen-vectors for non-zero eigen-values) which are part of Chevalley basis is given by  $\Phi = \{e_{i,j} \mid 1 \leq i \neq j \leq l+1\}$ . We fix a simple root system  $\Pi = \{e_{i,i+1} \mid 1 \leq i \leq l\}$ . A Chevalley basis is obtained by taking union of  $\Phi$  with the set  $\{[e_{i,i+1}, e_{i+1,i}] \mid i \leq i \leq l\}$ .

Thus the generators for the intermediate Chevalley group of type  $A_l$  over field  $K$  are  $x_{i,j}(t) = I + te_{i,j}$  where  $i \neq j$  and  $t \in K$ . Hence  $\bar{G} = \text{SL}(l+1, K)$  and the adjoint group is  $A_l(K) \cong \text{PSL}(l+1, K)$ .

**Type  $B_l$  :** The  $B_l$  type complex Lie algebra is  $o_{2l+1}(\mathbb{C}) = \{X \in M(2l+1, \mathbb{C}) \mid {}^T X \beta + \beta X = 0\}$  where  $\beta$  is as in the Section 3. Any  $X \in o_{2l+1}(\mathbb{C})$  is of the form  $\begin{pmatrix} 0 & X_{01} & X_{02} \\ -2{}^T X_{02} & X_{11} & X_{12} \\ -2{}^T X_{01} & X_{21} & -{}^T X_{11} \end{pmatrix}$  where  $X_{12}$  and  $X_{21}$  are skew-symmetric matrices of size  $l \times l$ .

The set of diagonal matrices give a Cartan subalgebra and the Cartan decomposition

gives us a Chevalley basis. Thus the roots in this case are  $\Phi = \{e_{i,j} - e_{-j,-i}, -e_{-i,-j} + e_{j,i}, e_{i,-j} - e_{j,-i}, e_{-i,j} - e_{-j,i}, 2e_{i,0} - e_{0,-i}, -2e_{-i,0} + e_{0,i} \mid 1 \leq i < j \leq l\}$ . The simple roots are  $\Pi = \{e_{i,i+1} - e_{-(i+1),-i}, 2e_{l,0} - e_{0,-l} \mid 1 \leq i \leq l-1\}$ .

In this case the intermediate Chevalley group is  $\Omega_{2l+1}(K)$  generated by the Chevalley generators: For  $1 \leq i, j \leq l$ ,

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}) && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(-e_{-i,j} + e_{-j,i}) && \text{for } i < j, \\ x_{i,0}(t) &= I + t(2e_{i,0} - e_{0,-i}) - t^2 e_{i,-i}, \\ x_{0,i}(t) &= I + t(-2e_{-i,0} + e_{0,i}) - t^2 e_{-i,i}. \end{aligned}$$

The adjoint group is  $B_l(K) \cong P\Omega_{2l+1}(K)$ .

**Type  $C_l$  :** The complex Lie algebra of type  $C_l$  is  $sp_{2l}(\mathbb{C}) = \{X \in M(2l, \mathbb{C}) \mid {}^T X \beta + \beta X = 0\}$  where  $\beta$  is as in Section 3. Any  $X \in sp_{2l}(\mathbb{C})$  is of the form  $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & -{}^T X_{11} \end{pmatrix}$  where  $X_{12}$  and  $X_{21}$  are symmetric matrices. The set of diagonal matrices is a Cartan subalgebra and the Cartan decomposition gives a Chevalley basis. The roots in this case are  $\{e_{i,j} - e_{-j,-i}, -e_{-i,-j} + e_{j,i}, e_{i,-j} + e_{j,-i}, e_{-i,j} + e_{-j,i}, e_{i,-i}, e_{-i,i} \mid 1 \leq i < j \leq l\}$ . The simple roots are  $\Pi = \{e_{i,(i+1)} - e_{-(i+1),-i}, e_{l,-l} \mid 1 \leq i \leq l-1\}$ .

The root generators for the group over a field  $K$  are: For  $1 \leq i, j \leq l$

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} + e_{j,-i}) && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} + e_{-j,i}) && \text{for } i < j, \\ x_{i,-i}(t) &= I + t e_{i,-i}, \\ x_{-i,i}(t) &= I + t e_{-i,i} \end{aligned}$$

which generate the intermediate Chevalley group  $\text{Sp}(2l, K)$ . The adjoint group is  $C_l(K) \cong \text{PSp}(2l, K)$ .

**Type  $D_l$  :** The  $D_l$  type complex Lie algebra is  $o_{2l}(\mathbb{C}) = \{X \in M_{2l}(\mathbb{C}) \mid {}^T X \beta + \beta X = 0\}$  where  $\beta$  is as in Section 3. Any  $X \in o_{2l}(\mathbb{C})$  is of the form  $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & -{}^T X_{11} \end{pmatrix}$  where  $X_{12}$  and  $X_{21}$  are skew-symmetric matrices. The set of diagonal matrices form a Cartan subalgebra. The roots in this case are  $\{e_{i,j} - e_{-j,-i}, -e_{-i,-j} + e_{j,i}, e_{i,-j} - e_{j,-i}, e_{-i,j} - e_{-j,i} \mid 1 \leq i < j \leq l\}$ . The simple roots are  $\Pi = \{e_{i,(i+1)} - e_{-(i+1),-i}, p_l = e_{(l-1),-l} - e_{l,-(l-1)} \mid 1 \leq i \leq l-1\}$ . This gives us a Chevalley basis.

The intermediate Chevalley group in this case is  $\Omega_{2l}(K)$  generated by the Chevalley generators: For  $1 \leq i, j \leq l$

$$\begin{aligned} x_{i,j}(t) &= I + t(e_{i,j} - e_{-j,-i}) && \text{for } i \neq j, \\ x_{i,-j}(t) &= I + t(e_{i,-j} - e_{j,-i}) && \text{for } i < j, \\ x_{-i,j}(t) &= I + t(e_{-i,j} - e_{-j,i}) && \text{for } i < j. \end{aligned}$$

The adjoint group is  $D_l(K) \cong P\Omega_{2l}(K)$ .

## 5. DESCRIPTION OF AUTOMORPHISM GROUP OF CLASSICAL GROUPS

To build a MOR cryptosystem we need to work with the automorphism group of Chevalley groups. In this section we describe the automorphism group of classical groups following Dieudonne [8]. Let  $G$  be one of the following groups: adjoint or intermediate Chevalley group of classical type or more generally the groups listed in the table in section 4.1.

**Conjugation Automorphisms:** For  $t \in G$  the map given by  $g \mapsto tgt^{-1}$  is an automorphism of  $G$ , called an **inner automorphism**. More generally if  $G$  is a normal subgroup of  $N$  then the conjugation maps  $g \mapsto ngn^{-1}$  for  $n \in N$  are called conjugation automorphisms of  $G$ .

**Central Automorphisms:** Let  $\chi: G \rightarrow \mathcal{Z}(G)$  be a group homomorphism to the center of the group. Then the map  $g \mapsto \chi(g)g$  is an automorphism of  $G$ , known as the central automorphism. There are no non-trivial central automorphisms for perfect groups, for example, the adjoint Chevalley groups  $SL(l+1, K)$  and  $Sp(2l, K)$ ,  $K \geq 4$  and  $l \geq 2$ . In case of orthogonal group, the center is of two elements  $\{I, -I\}$ . Any map  $\chi$  maps  $\Omega_d(K)$  to identity. This implies that there are at most four central automorphisms in this case.

**Field Automorphisms:** Let  $f \in \text{Aut}(K)$ . Then the map  $x_r(t) \mapsto x_r(f(t))$  for all  $r \in \Phi$  and  $t \in K$  extends to an automorphism of  $G$ . These are called field automorphism. In terms of matrices these amount to replacing each term of the matrix by its image under  $f$ .

**Graph Automorphisms:** A symmetry of Dynkin diagram induces such automorphisms. This way we get automorphisms of order 2 for  $A_l(K), l \geq 2$  and  $D_l(K), l \geq 4$ . We also get an automorphisms of order 3 for  $D_4(K)$ . This map is given by  $x_r(t) \mapsto x_{\bar{r}}(\gamma_r t)$  where  $r \mapsto \bar{r}$  is Dynkin diagram automorphism and  $\gamma_r = \pm 1$ .

In the case of  $A_l$  for  $l \geq 2$ , the map  $x \mapsto A^{-1}Tx^{-1}A$  where

$$A = \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & -1 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & \cdots & -1 & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ (-1)^{l-1} & \cdots & 0 & 0 & 0 & 0 \end{pmatrix}$$

explicitly describes the graph automorphism.

In the case of  $D_l$  for  $l \geq 5$ , the graph automorphism is given by  $x \mapsto B^{-1}xB$  where  $B$  is a permutation matrix obtained from identity matrix of size  $2l \times 2l$  by switching the  $l^{\text{th}}$  row and  $-l^{\text{th}}$  row. This automorphism is a conjugating automorphism.

**Theorem 5.1** (Dieudonne). *Let  $K$  be a field of odd characteristic and  $l \geq 2$ .*

- (1) *For the group  $SL(l+1, K)$  any automorphism is of the form  $\iota\gamma\theta$  where  $\iota$  is a conjugation automorphism defined by elements of  $GL(l+1, K)$  and  $\gamma$  is a graph automorphism of  $A_l$  type.*
- (2) *For the group  $O(d, K)$  any automorphism is of the form  $c_\chi\iota\theta$  where  $c_\chi$  is a central automorphism,  $\iota$  a conjugation automorphism by  $GO(d, K)$  elements (this includes the graph automorphism of  $D_l$  case).*
- (3) *For the group  $Sp(2l, K)$  any automorphism is of the form  $\iota\theta$  where  $\iota$  is a conjugation automorphism by  $GSp(2l, K)$  elements.*

In all cases  $\theta$  denotes field automorphisms.

In the above theorem, conjugation automorphisms are given by conjugation by elements of a larger group and it includes the group of inner automorphisms. We introduce diagonal automorphisms to make it more precise. The conjugation automorphisms  $\iota$  can be written as a product of  $\iota_g$  and  $\delta$  where  $\iota_g$  is an inner automorphism and  $\delta$  is a diagonal automorphism.

**Diagonal Automorphisms:** The adjoint Chevalley group  $\mathcal{L}(K)$  is normalized by  $\hat{H}$  which is a subgroup of  $\text{Aut}(\mathcal{L}_K)$ . Thus for  $h(\chi) \in \hat{H}$  which is not in  $H$  gives an automorphism  $g \rightarrow h(\chi)gh(\chi)^{-1}$  (which is not an inner automorphism). Such automorphisms are called diagonal automorphism. The explicit action on generators is as follows:  $h(\chi)x_r(t)h(\chi)^{-1} = x_r(\chi(r)t)$ . The group  $\hat{G}$  is identified in [20, Chapter III, Section 6] with corresponding similitude group. In the case of  $A_l$  the diagonal automorphisms are given by conjugation by diagonal elements of  $\text{PGL}(l+1, q)$  on  $A_l(q) = \text{PSL}(l+1, q)$ . In the case of  $B_l, C_l$  and  $D_l$  the diagonal automorphisms are given by conjugation by the corresponding diagonal group defined in Section 3.5.

Let  $K$  be a finite field of odd characteristic and  $G = \mathcal{L}(K)$  be an adjoint Chevalley group over  $K$  as defined in Section 4. Steinberg described the automorphisms of these groups. We have the following theorem [5, Theorem 12.5.1] and [22],

**Theorem 5.2** (Steinberg). *Let  $G = \mathcal{L}(K)$  where  $\mathcal{L}$  is simple and  $K (= \mathbb{F}_q)$  is a finite field. Let  $\phi \in \text{Aut}(G)$ . Then there exist inner, diagonal, graph and field automorphisms, denoted by  $\iota, \delta, \gamma$  and  $\theta$  respectively, such that  $\phi = \iota\delta\gamma\theta$ .*

The automorphism groups of Chevalley groups over certain rings have been studied by Bunina [3, 4].

## 6. SOLVING THE WORD PROBLEM IN $G$

We work with a finite field  $K = \mathbb{F}_q$  of odd characteristic. Let  $G$  be one of the following groups:  $\text{SL}(l+1, q)$ ,  $\text{O}(2l+1, q)$ ,  $\text{Sp}(2l, q)$  or  $\text{O}(2l, q)$  for  $l \geq 2$ . Following the notation from the theory of Chevalley groups we also call them  $A_l, B_l, C_l$  or  $D_l$  type respectively. We know that the group  $G$  is generated by Chevalley generators listed in the Section 3.1. In fact, there are finite presentations for these groups due to Steinberg. In computational group theory, one is always looking for algorithms that solve the word problem. Algorithms for word problem are useful in other programs in computational group theory, such as, the group recognition program and studying the membership problems in finite groups. Extensive work on these programs are being done by several people, most notably of those are Leedham-Green and O'Brien [16] and Guralnick et. al. [10–12]. We need an (efficient) algorithm to write an element  $g \in G$  as a product of generators, i.e., a solution to the word problem for an efficient implementation of the MOR cryptosystem.

In the case of groups of  $A_l$  type, i.e., when  $G$  is a special linear group, one has the well-known algorithm, the row-column operations. One observes that the effect of multiplying by a Chevalley generator on a matrix from left or right is either a row or a column operation respectively. Using this algorithm one can start with any matrix  $g \in \text{SL}(l+1, q)$  and get the identity matrix thus writing  $g$  as a product of generators. One of the objective in this paper is to develop a similar algorithm for the groups of type  $B_l, C_l$  and  $D_l$  type.

In general, one has the Bruhat decomposition for Chevalley groups which can be used to write any element in a normal form. Every element  $g \in \mathcal{L}(K)$  has a unique expression [5,

Corollary 8.4.4]  $u_1 h n_w u$  where  $u_1 \in U, h \in H, w \in W$  and  $u \in U_w^-$ . Here we fixed a coset representative for each  $w \in W$  and denote it by  $n_w$ . The element  $n := h n_w$  belongs to  $N$ .

Thus, the main objective of this section is to give an algorithm, in a similar line as the row-column operations for  $A_l$ , to solve the word problem for other Chevalley groups.

Cohen, Murray and Taylor [7] proposed a generalized algorithm using the row-column operations, using a representation of Chevalley groups. The key idea there was to bring down an element to a maximal parabolic subgroup and repeat the process inductively. Here we use the natural matrix representation of these groups. Thus our algorithm is more direct and works with matrices explicitly and effectively. A novelty of our algorithm is that we do not need to assume that the Chevalley generators generate the group under consideration. Thus our algorithm proves independently the fact that these groups are generated by those generators.

**6.1. An algorithm for row-column operations for the groups of Lie type  $C_l$  and  $D_l$ .** First we will deal with groups of  $C_l$  and  $D_l$  type. That is, we work with groups  $\text{Sp}(2l, q)$  and  $\text{O}(2l, q)$ . The Chevalley generators are described in Section 3.1. In general, we have three kind of Chevalley generators. For  $1 \leq i, j \leq l$

CG1:  $\begin{pmatrix} R & \\ & {}^t R^{-1} \end{pmatrix}$  where  $R = I + t e_{i,j}; i \neq j$ .

CG2:  $\begin{pmatrix} I & R \\ & I \end{pmatrix}$  where  $R$  is either  $t(e_{i,-j} + e_{j,-i})$  or  $t e_{i,-i}$  in the case of  $C_l$  and  $R$  is  $t(e_{i,-j} - e_{j,-i})$  in the case of  $D_l$ .

CG3:  $\begin{pmatrix} I & \\ R & I \end{pmatrix}$  where  $R$  is either  $t(e_{-i,j} + e_{-j,i})$  or  $t e_{-i,i}$  in the case of  $C_l$  and  $R$  is  $t(e_{-i,j} - e_{-j,i})$  in the case of  $D_l$ .

Let  $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$  be a  $2l \times 2l$  matrix. Let us note the effect of multiplying  $g$  by elements from above.

$$\begin{aligned}
CG1: \quad & \begin{pmatrix} R & \\ & {}^t R^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} RA & RB \\ {}^t R^{-1}C & {}^t R^{-1}D \end{pmatrix} \\
& \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} R & \\ & {}^t R^{-1} \end{pmatrix} = \begin{pmatrix} AR & B {}^t R^{-1} \\ CR & D {}^t R^{-1} \end{pmatrix}. \\
CG2: \quad & \begin{pmatrix} I & R \\ & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A + RC & B + RD \\ C & D \end{pmatrix} \\
& \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & R \\ & I \end{pmatrix} = \begin{pmatrix} A & AR + B \\ C & CR + D \end{pmatrix}. \\
CG3: \quad & \begin{pmatrix} I & \\ R & I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ RA + C & RB + D \end{pmatrix} \\
& \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & \\ R & I \end{pmatrix} = \begin{pmatrix} A + BR & B \\ C + DR & D \end{pmatrix}.
\end{aligned}$$

**6.1.1. Algorithm.** We produce a brief overview of the row-column operations for groups of type  $\text{Sp}(2l, q)$  and  $\text{O}(2l, q)$ .

Step 1: **Input:** A matrix  $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$  which belongs to  $\text{Sp}(2l, q)$  or  $\text{O}(2l, q)$ .

**Output:** The matrix  $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$  is one of the following kind:

- a: The matrix  $C_1$  is a diagonal matrix  $\text{diag}(1, 1, \dots, 1, \lambda)$  and  $A_1$  is  $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & a_{22} \end{pmatrix}$  where  $A_{11}$  is symmetric in the  $\text{Sp}(2l, q)$  case and skew-symmetric in the  $\text{O}(2l, q)$  case of size  $l-1$ . Furthermore,  $A_{12} = \lambda^T A_{21}$  in the  $\text{Sp}(2l, q)$  case and  $A_{12} = -\lambda^T A_{21}$  in the  $\text{O}(2l, q)$  case.
- b: The matrix  $C_1$  is a diagonal matrix  $\text{diag}(1, 1, \dots, 1, 0, \dots, 0)$  with number of 1s equal to  $m$  and  $A_1$  looks like  $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$  where  $A_{11}$  is an  $m \times m$  symmetric in the  $\text{Sp}(2l, q)$  case and skew-symmetric in the  $\text{O}(2l, q)$  case.
- c: The matrices  $B_1$  and  $D_1$  are  $l \times l$ .

**Justification.** : Observe that the effect of CG1 on  $C$  is the usual row-column operations. Thus we can reduce  $C$  to the diagonal form and Corollary 6.2 makes sure that  $A$  has required form.

Step 2: **Input:** matrix  $g_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ .

**Output:** matrix  $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$ ;  $A_2$  is a diagonal matrix  $\text{diag}(1, 1, \dots, 1, \lambda)$ .

**Justification:** Observe the effect of CG2. It changes  $A_1$  by  $A_1 + RC_1$ . Using Lemma 6.5 we can make the matrix  $A_1$  the zero matrix in the first case and  $A_{11}$  the zero matrix in the second case. After that we make use of Lemma 6.6 to interchange the rows so that we get zero matrix at the place of  $C_1$ . If required use CG1 to make  $A_1$  a diagonal matrix. The Lemma 6.4 ensures that  $D_1$  becomes  ${}^T A_2^{-1}$ .

Step 3: **Input:** matrix  $g_2 = \begin{pmatrix} A_2 & B_2 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$ ;  $A_2$  is a diagonal matrix  $\text{diag}(1, \dots, 1, \lambda)$ .

**Output:** Matrix  $g_3 = \begin{pmatrix} A_2 & 0 \\ 0 & {}^T A_2^{-1} \end{pmatrix}$ ;  $A_2$  is diagonal matrix  $\text{diag}(1, 1, \dots, 1, \lambda)$ .

**Justification:** Using Corollary 6.3 we see that the matrix  $B_2$  has certain form. We can use CG2 to make the matrix  $B_2$  a zero matrix because of Lemma 6.5.

Step 4: **Input:** matrix  $g_3 = \text{diag}(1, \dots, 1, \lambda, 1, \dots, 1, \lambda^{-1})$ .

**Output:** Identity matrix

**Justification:** In the case of  $\text{Sp}(2l, q)$  the diagonal matrix can be written as a product of generators by first part of Lemma 6.7. In the case of  $\text{O}(2l, q)$ , using second part of Lemma 6.7 we can reduce to  $\text{diag}(1, \dots, 1, \zeta, 1, \dots, 1, \zeta^{-1})$  where  $\zeta$  is a fixed non-square in  $\mathbb{F}_q$ . Thus multiplying with  $d(\zeta)^{-1}$  we get the result.

**6.2. Time-complexity of the above algorithm.** We establish that the time-complexity of the above algorithm is  $\mathcal{O}(l^3)$ .

In Step 1, we are making  $C$  a diagonal matrix by row-column operations. That has complexity  $\mathcal{O}(l^3)$ .

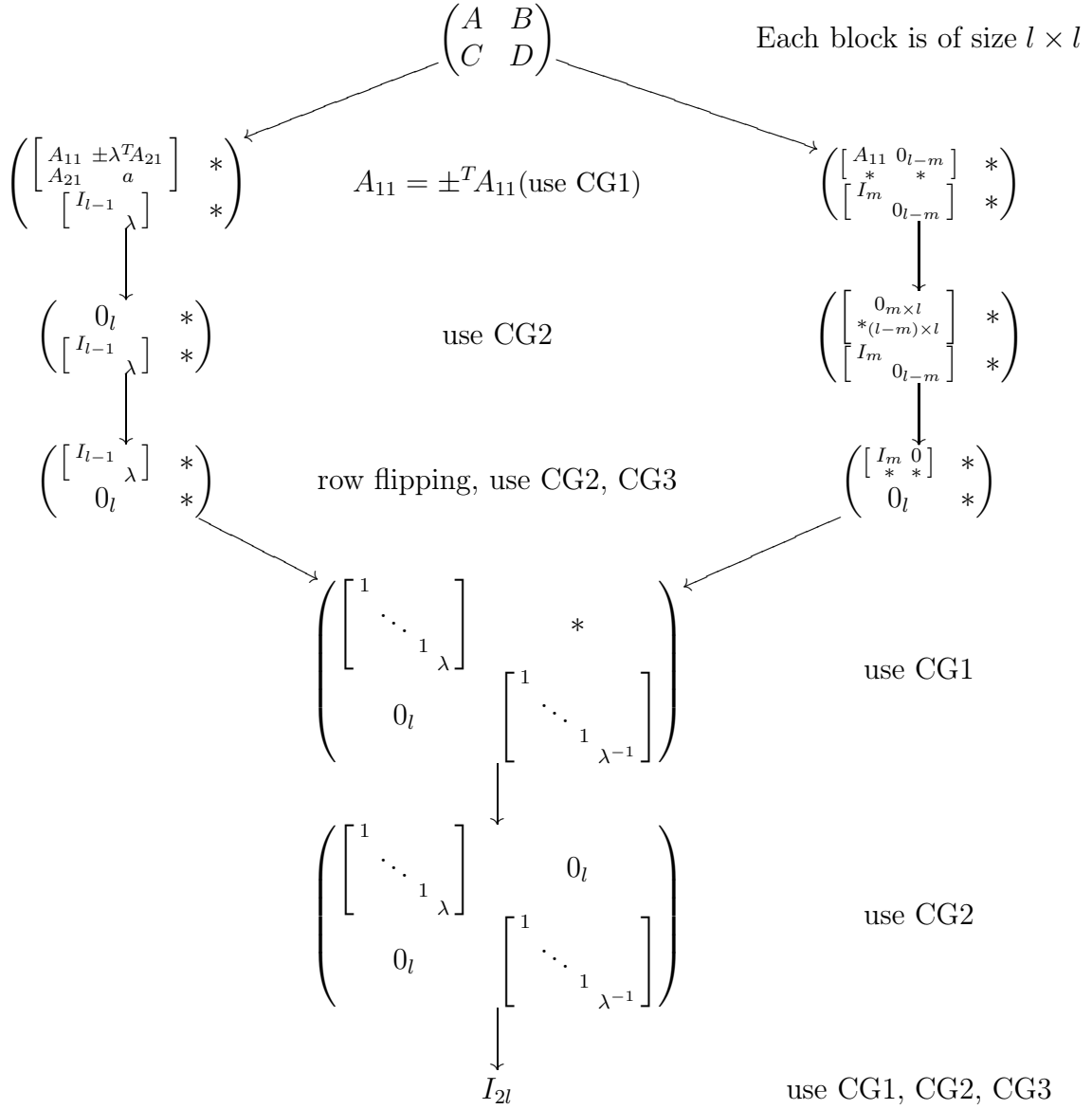
In Step 2,  $A_1 + RC_1$  is two field multiplications and two additions. In the worst case, it has to be done  $l^2$  times and so the complexity is  $\mathcal{O}(l^2)$ .

Step 3 is similar to Step 2 above and has complexity  $\mathcal{O}(l^2)$ .

Step 4 has only a few steps that is independent of  $l$ .

Then clearly, the time-complexity of our algorithm is  $\mathcal{O}(l^3)$ .

**6.3. Flowchart of the above algorithm.** The input to the algorithm is a  $2l \times 2l$  matrix in  $\text{Sp}(2l, q)$  or  $\text{O}(2l, q)$  represented as blocks of size  $l$ .



**6.4. Useful lemmas.** In this section we set notation and prove lemmas which were used (and will be used) to justify the above algorithm (and the later algorithm). Some of these might be well known to experts but we include them here for the convenience of the reader. We make use of the following while computing with matrices:

$$e_{i,j}e_{k,l} = \delta_{jk}e_{i,l} \text{ where } \delta_{jk} \text{ is the Kronecker delta.}$$

**Lemma 6.1.** *Let  $Y = \text{diag}(1, \dots, 1, \lambda, \dots, \lambda)$  of size  $l$  with number of 1s equal to  $m < l$ . Let  $X$  be a matrix such that  $YX$  is symmetric (skew-symmetric) then  $X$  is of the form  $\begin{pmatrix} X_{11} & \lambda^T X_{21} \\ X_{21} & X_{22} \end{pmatrix}$  where  $X_{11}$  is symmetric (skew symmetric) and  $X_{12} = \lambda^T X_{21}$  ( $X_{12} = -\lambda^T X_{21}$ ).*

*Proof.* We observe that the matrix  $YX = \begin{pmatrix} X_{11} & X_{12} \\ \lambda X_{21} & \lambda X_{22} \end{pmatrix}$ . The condition that  $YX$  is symmetric implies  $X_{11}$  (and  $X_{22}$  if  $\lambda \neq 0$ ) is symmetric and  $X_{12} = \lambda^T X_{21}$ . •

**Corollary 6.2.** Let  $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$  be either in  $Sp(2l, q)$  or  $O(2l, q)$ .

- (1) If  $C$  is a diagonal matrix  $\text{diag}(1, 1, \dots, 1, 0, \dots, 0)$  with number of 1s equal to  $m < l$  then the matrix  $A$  has to be of the form  $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$  where  $A_{11}$  is an  $m \times m$  symmetric if  $g$  is symplectic and is skew-symmetric if  $g$  is orthogonal.
- (2) If  $C$  is a diagonal matrix  $\text{diag}(1, 1, \dots, 1, \lambda)$  then the matrix  $A$  has to be of the form  $\begin{pmatrix} A_{11} & \lambda^T A_{21} \\ A_{21} & A_{22} \end{pmatrix}$  where  $A_{11}$  is an  $(l-1) \times (l-1)$  symmetric if  $g$  is symplectic and is skew-symmetric if  $g$  is orthogonal.

*Proof.* We use the condition that  $g$  satisfies  ${}^T g \beta g = \beta$ .

$$\begin{aligned} {}^T g \beta g &= \begin{pmatrix} {}^T A & {}^T C \\ {}^T B & {}^T D \end{pmatrix} \begin{pmatrix} I \\ \pm I \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} \pm {}^T C & {}^T A \\ \pm {}^T D & {}^T B \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \pm {}^T C A + {}^T A C & * \\ * & * \end{pmatrix} \end{aligned}$$

This gives  $\pm {}^T C A + {}^T A C = 0$  which means  $CA$  is symmetric (note  $C = {}^T C$  as  $C$  is diagonal) if  $g$  is symplectic and is skew-symmetric if  $g$  is orthogonal. The Lemma 6.1 gives the required form for  $A$ . •

**Corollary 6.3.** Let  $g = \begin{pmatrix} A & B \\ 0 & A^{-1} \end{pmatrix}$  where  $A = \text{diag}(1, \dots, 1, \lambda)$  be an element of either  $Sp(2l, q)$  or  $O(2l, q)$  then the matrix  $B$  is of the form  $\begin{pmatrix} B_{11} & \lambda^T B_{21} \\ B_{21} & B_{22} \end{pmatrix}$  where  $B_{11}$  is a symmetric matrix of size  $l-1$  if  $g$  is symplectic and is skew-symmetric if  $g$  is orthogonal.

*Proof.* Yet again, we use the condition that  $g$  satisfies  ${}^T g \beta g = \beta$  and  $A = {}^T A$ .

$$\begin{aligned} {}^T g \beta g &= \begin{pmatrix} A & B \\ {}^T B & A^{-1} \end{pmatrix} \begin{pmatrix} I \\ \pm I \end{pmatrix} \begin{pmatrix} A & B \\ A^{-1} \end{pmatrix} \\ &= \begin{pmatrix} A & B \\ \pm A^{-1} & {}^T B \end{pmatrix} \begin{pmatrix} A & B \\ A^{-1} \end{pmatrix} = \begin{pmatrix} I & \\ \pm I & \pm A^{-1} B + {}^T B A^{-1} \end{pmatrix} \end{aligned}$$

This gives  $\pm A^{-1} B + {}^T B A^{-1} = 0$  which means  $A^{-1} B$  is symmetric if  $g$  is symplectic and is skew-symmetric if  $g$  is orthogonal. Then Lemma 6.1 gives the required form for  $B$ . •

**Lemma 6.4.** Let  $g = \begin{pmatrix} A & * \\ 0 & D \end{pmatrix} \in GL(2l, q)$ . If  $g$  belongs to  $Sp(2l, q)$  or  $O(2l, q)$  then  $D = {}^T A^{-1}$ .

*Proof.* We use  ${}^T g \beta g = \beta$ .

$$\begin{aligned} \begin{pmatrix} I \\ \pm I \end{pmatrix} &= \beta = {}^T g \beta g = \begin{pmatrix} {}^T A & 0 \\ * & {}^T D \end{pmatrix} \begin{pmatrix} I \\ \pm I \end{pmatrix} \begin{pmatrix} A & * \\ 0 & D \end{pmatrix} \\ &= \begin{pmatrix} 0 & {}^T A \\ \pm {}^T D & * \end{pmatrix} \begin{pmatrix} A & * \\ 0 & D \end{pmatrix} = \begin{pmatrix} 0 & {}^T A D \\ \pm {}^T D A & * \end{pmatrix} \end{aligned}$$

This gives  ${}^T A D = I$ . •



**Lemma 6.5.** Let  $Y = \text{diag}(1, 1, \dots, 1, \lambda)$  be of size  $l$  where  $\lambda \neq 0$  and  $X = (x_{ij})$  be a matrix such that  $YX$  is symmetric (skew-symmetric). Then  $X = (R_1 + R_2 + \dots)Y$  where each  $R_m$  is of the form  $t(e_{i,j} + e_{j,i})$  for some  $i < j$  or of the form  $te_{i,i}$  for some  $i$  (in the case of skew-symmetric each  $R_m$  is of the form  $t(e_{i,j} - e_{j,i})$  for some  $i < j$ ).

*Proof.* Since  $YX$  is symmetric, the matrix  $X$  is of the following form (see Lemma 6.1):  $\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & x_{nn} \end{pmatrix}$  where  $X_{11}$  is symmetric and  $X_{21}$  is a row of size  $l-1$  ( $x_{l1}x_{l2} \dots x_{l,l-1}$ ) and  $X_{12} = \lambda^T X_{21}$ . Clearly any such matrix is sum of the matrices of the form  $RY$ . A similar calculation proves the result in the skew-symmetric case.  $\bullet$

We need certain Weyl group elements which can be used for switching rows.

**Lemma 6.6.** With the indexing of basis as  $1, \dots, l, -1, \dots, -l$ , for any matrix  $g$  in  $Sp(2l, q)$  or  $O(2l, q)$ , the  $i^{\text{th}}$  row can be interchanged with  $-i^{\text{th}}$  row with possibly a sign change. Further, we can do the same in  $O(2l+1, q)$ .

*Proof.* For the symplectic group  $Sp(2l, q)$  consider the following root generators:  $x_{i,-i} = I + e_{i,-i}$  and  $y_{i,-i} = I - e_{-i,i}$ . Then the element  $w_{i,-i} = x_{i,-i}y_{i,-i}x_{i,-i}$  is in the Weyl group and multiplication by this element to a matrix  $g$  has desired property.

$$\begin{aligned} w_{i,-i} &= x_{i,-i}y_{i,-i}x_{i,-i} = (I + e_{i,-i})(I - e_{-i,i})(I + e_{i,-i}) \\ &= (I + e_{i,-i} - e_{-i,i} - e_{i,i})(I + e_{i,-i}) \\ &= I + e_{i,-i} - e_{-i,i} - e_{i,i} - e_{-i,-i}. \end{aligned}$$

In the matrix form:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ -1 & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} & & & 1 \\ & & 1 & \\ -1 & & & \\ & & & 1 \end{pmatrix}.$$

For the orthogonal group  $O(2l, q)$  consider the following root generators:  $x_{ij} = I + (e_{i,-j} - e_{j,-i})$  and  $y_{ij} = I + (e_{-i,j} - e_{-j,i})$  for  $i < j$ . Then the element  $w_{ij} = x_{ij}y_{ij}x_{ij}$  is in the Weyl group and multiplication by this element to a matrix  $g$  changes  $i^{\text{th}}$  row with  $-j^{\text{th}}$  row with a sign change and  $j^{\text{th}}$  row with  $-i^{\text{th}}$  row with a sign change simultaneously.

$$\begin{aligned} w_{ij} &= x_{ij}y_{ij}x_{ij} = (I + e_{i,-j} - e_{j,-i})(I + e_{-i,j} - e_{-j,i})(I + e_{i,-j} - e_{j,-i}) \\ &= (I + e_{-i,j} - e_{-j,i} + e_{i,-j} + e_{i,-j}e_{-i,j} - e_{i,-j}e_{-j,i} - e_{j,-i} - e_{j,-i}e_{-i,j} \\ &\quad + e_{j,-i}e_{-j,i})(I + e_{i,-j} - e_{j,-i}) \\ &= (I + e_{-i,j} - e_{-j,i} + e_{i,-j} - e_{i,i} - e_{j,-i} - e_{j,j})(I + e_{i,-j} - e_{j,-i}) \\ &= I - e_{i,i} - e_{j,j} - e_{-i,-i} - e_{-j,-j} + e_{i,-j} - e_{j,-i} + e_{-i,j} - e_{-j,i}. \end{aligned}$$

In the matrix form:

$$\begin{pmatrix} 1 & & & 1 \\ & 1 & -1 & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ -1 & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & 1 \\ & 1 & -1 & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ -1 & & & \end{pmatrix}.$$

Also since  $GL(l, q)$  embeds inside  $O(2l, q)$  via  $A \mapsto \begin{pmatrix} A & \\ & T_{A^{-1}} \end{pmatrix}$  the CG1 generators generate the subgroup  $SL(l, q)$  and we have corresponding Weyl group elements,  $\sigma_{ij} = I -$

$e_{i,i}-e_{j,j}+e_{i,j}-e_{j,i}-e_{-i,-i}-e_{-j,-j}+e_{-i,-j}-e_{-j,-i}$  which interchanges  $i^{\text{th}}$  to  $j^{\text{th}}$  row and  $-i^{\text{th}}$  to  $-j^{\text{th}}$  row simultaneously with a sign change. We have the extra generator  $w_l \in O(2l, q)$  which interchanges  $l^{\text{th}}$  row with  $-l^{\text{th}}$  row with a sign change. We can compute and check that  $w_{l-1} = w_l \sigma_{l,l-1} w_{l,l-1} = I - e_{l-1,l-1} - e_{-(l-1),-(l-1)} - e_{(l-1),-(l-1)} - e_{-(l-1),(l-1)}$  which interchanges  $l-1^{\text{th}}$  row with  $-(l-1)^{\text{th}}$  row (possibly with a sign change) and inductively we can produce  $w_i$  which interchanges  $i^{\text{th}}$  row with  $-i^{\text{th}}$  row possibly with a sign change. In the matrix form:

$$\begin{aligned} w_3 \sigma_{23} w_{23} &= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & -1 \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & & & -1 \\ & & 1 & \\ & & & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & & & \\ & 1 & & -1 \\ & & 1 & \\ & -1 & & 1 \end{pmatrix} = w_2. \end{aligned}$$

Further notice that  $O(2l, q)$  is embedded inside  $O(2l+1, q)$ . Thus we can do the same in  $O(2l+1, q)$  as well. •

- Lemma 6.7.** (1) In the case of  $Sp(2l, q)$ , the element  $\text{diag}(\underbrace{1, \dots, 1}_l, \underbrace{1, \dots, 1}_l, \lambda^{-1})$  is a product of Chevalley generators.
- (2) In the case of  $O(2l, q)$ , the element  $\text{diag}(\underbrace{1, \dots, 1}_l, \underbrace{1, \dots, 1}_l, \lambda^{-1})$  is a product of Chevalley generators where  $\lambda \in \mathbb{F}_q^{\times 2}$ .
- (3) In the case of  $O(2l+1, q)$  diagonal elements  $\text{diag}(\underbrace{1, \dots, 1}_l, \underbrace{1, \dots, 1}_l, \lambda^{-1})$  where  $\lambda \in \mathbb{F}_q^{\times 2}$  and  $\text{diag}(-1, 1, \dots, 1)$  are a product of Chevalley generators.

*Proof.* In the case of  $Sp(2l, q)$ , we compute  $w_{l,-l}(t) = (I + te_{l,-l})(I - t^{-1}e_{-l,l})(I + te_{l,-l}) = I - e_{l,l} - e_{-l,-l} + te_{l,-l} - t^{-1}e_{-l,l}$  and then compute  $h_l(\lambda) = w_{l,-l}(\lambda)w_{l,-l}(-1)$  which is the required element.

In the case of  $O(2l, q)$ , we compute  $w_{l-1,-l}(t) = (I + te_{l-1,-l} - te_{l,-(l-1)})(I + t^{-1}e_{-(l-1),l} - t^{-1}e_{-l,l-1})(I + te_{l-1,-l} - te_{l,-(l-1)}) = I + t^{-1}e_{-(l-1),l} - e_{-(l-1),-(l-1)} - t^{-1}e_{-l,l-1} - e_{-l,-l} + te_{l-1,-l} - e_{l-1,l-1} - te_{l,-(l-1)} - e_{l,l}$  and

$$h_{l-1,-l}(t) = w_{l-1,-l}(t)w_{l-1,-l}(-1) = \text{diag}(\underbrace{1, \dots, 1}_l, \underbrace{1, \dots, 1}_l, t^{-1}, t^{-1})$$

. Similarly we compute  $\sigma_{l-1,l}(t) = (I + te_{l-1,l} + te_{-l,-(l-1)})(I - t^{-1}e_{l,l-1} - t^{-1}e_{-(l-1),-l})(I + te_{l-1,l} + te_{-l,-(l-1)})$  and  $h_{l-1,l}(t) = \sigma_{l-1,l}(t)\sigma_{l-1,l}(-1) = \text{diag}(\underbrace{1, \dots, 1}_l, \underbrace{1, \dots, 1}_l, t^{-1}, t^{-1})$ .

In the matrix form:

$$\begin{aligned}
w_{2,-3}(t) &= \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & -t & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & -t^{-1} & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & -t & \\ & & & & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & -t & \\ & & & & 1 \\ -t^{-1} & & t^{-1} & & 0 \end{pmatrix}.
\end{aligned}$$

and

$$\begin{aligned}
h_{2,-3}(t) = w_{2,-3}(t)w_{2,-3}(-1) &= \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & -t & \\ & & & & 1 \\ -t^{-1} & & t^{-1} & & 0 \end{pmatrix} \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 1 & \\ & & & & -1 \\ 1 & & -1 & & 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & & & & \\ & t & & & \\ & & t & & \\ & & & 1 & \\ & & & & t^{-1} \\ & & & & & t^{-1} \end{pmatrix}.
\end{aligned}$$

Furthermore,

$$\sigma_{23}(t) = \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & -t^{-1} & & & \\ & & 1 & & \\ & & & 0 & -t^{-1} \\ & & & t & 0 \end{pmatrix} \text{ and } h_{23}(t) = \sigma_{23}(t)\sigma_{23}(-1) = \begin{pmatrix} 1 & & & & \\ & t & & & \\ & & t^{-1} & & \\ & & & 1 & \\ & & & & t^{-1} \\ & & & & & t \end{pmatrix}.$$

Thus multiplying  $h_{l-1,-l}(t)$  and  $h_{l-1,l}(t^{-1})$  we get the required result.

In the case of  $O(2l+1, q)$  we compute  $w_{l,0} = x_{l,0}(1)x_{0,l}(-1)x_{l,0}(1) = I - e_{-l,-l} - e_{-l,l} - e_{l,l} - 2e_{0,0} - e_{l,-l}$  and multiply it with  $w_l$  to get the required matrix.  $\bullet$

**Lemma 6.8.** Let  $g = \begin{pmatrix} \alpha & X & * \\ * & A & * \\ * & C & * \end{pmatrix}$  be in  $O(2l+1, q)$ .

- (1) If  $C = \text{diag}(1, \dots, 1, \lambda)$  and  $X = 0$  then  $A$  is of the form  $\begin{pmatrix} A_{11} & -\lambda^T A_{21} \\ A_{21} & a \end{pmatrix}$  with  $A_{11}$  skew-symmetric.
- (2) If  $C = \text{diag}(1, \dots, 1, 0, \dots, 0)$  with number of 1s equal  $m < l$  and  $X$  has first  $m$  entries 0 then  $A$  is of the form  $\begin{pmatrix} A_{11} & 0 \\ * & * \end{pmatrix}$  with  $A_{11}$  skew-symmetric.

*Proof.* We use the equation  ${}^Tg\beta g = \beta$  and get  $2{}^TXX = -(CA + {}^TAC)$ . In the first case  $X = 0$ , so we can use 6.2 to get required form for  $A$ . In the second case we note that  ${}^TXX$  has top-left block 0 and get the required form. •

**Lemma 6.9.** Let  $g = \begin{pmatrix} \alpha & X & Y \\ * & A & * \\ * & 0 & D \end{pmatrix}$  be in  $O(2l+1, q)$  then  $X = 0$  and  $D = {}^TA^{-1}$ .

*Proof.* We compute  ${}^Tg\beta g = \beta$  and get  $2{}^TXX = 0$  and  $2{}^TXY + {}^TAD = I$ . This gives the required result. •

**Lemma 6.10.** Let  $g = \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix}$ , with  $A$  an invertible diagonal matrix, be in  $O(2l+1, q)$  then  $\alpha^2 = 1, F = 0 = Y, D = A^{-1}$  and  ${}^TDB + {}^TBD = 0$ .

*Proof.*

$$\begin{aligned} {}^Tg\beta g &= \begin{pmatrix} \alpha & 0 & {}^TF \\ 0 & {}^TA & 0 \\ {}^TY & {}^TB & {}^TD \end{pmatrix} \begin{pmatrix} 2 & & \\ & I & \\ & & I \end{pmatrix} \begin{pmatrix} \alpha & 0 & Y \\ 0 & A & B \\ F & 0 & D \end{pmatrix} \\ &= \begin{pmatrix} 2\alpha^2 & {}^TFA & 2\alpha Y + {}^TFB \\ {}^TAF & 0 & {}^TAD \\ 2\alpha {}^TY + {}^TBF & {}^TDA & 2{}^TY Y + {}^TDB + {}^TBD \end{pmatrix}. \end{aligned}$$

Equating this with  $\beta$  we get the required result. •

**Lemma 6.11.** Let  $g = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & A & B \\ 0 & 0 & A^{-1} \end{pmatrix} \in O(2l+1, q)$  where  $A = \text{diag}(1, \dots, 1, \lambda)$  is invertible then  $B$  is of the form  $\begin{pmatrix} B_{11} & \lambda^{-1}{}^TB_{21} \\ B_{21} & b \end{pmatrix}$ .

*Proof.* This follows from the computation in the Lemma 6.10 that  $A^{-1}B + {}^TBA^{-1} = 0$  and Corollary 6.2. •

**6.5. An algorithm for row-column operations for the groups of Lie type  $B_l$ .** Here we work with the group  $O(2l+1, q)$ . Recall that the basis will be indexed by  $0, 1, \dots, l, -1, \dots, -l$ . The Chevalley generators are described in the Section 3.1. In general, we have four kind of Chevalley generators. For  $1 \leq i, j \leq l$

CG1:  $\begin{pmatrix} 1 & & \\ & R & \\ & & {}^TR^{-1} \end{pmatrix}$  where  $R = I + te_{i,j}; i \neq j$ .

CG2:  $\begin{pmatrix} 1 & & \\ & I & R \\ & & I \end{pmatrix}$  where  $R$  is  $t(e_{i,-j} - e_{j,-i}); i < j$ .

CG3:  $\begin{pmatrix} 1 & & \\ & I & \\ & R & I \end{pmatrix}$  where  $R$  is  $t(e_{-i,j} - e_{-j,i}); i < j$ .

CG4:  $I + t(2e_{i0} - e_{0,-i}) - t^2e_{i,-i}, I + t(-2e_{-i,0} + e_{0i}) - t^2e_{-i,i}$ .

We observe that CG1, CG2 and CG3 generate the subgroup  $O(2l, q)$  of  $O(2l + 1, q)$  given by  $x \mapsto \begin{pmatrix} 1 & & \\ & x & \\ & & \end{pmatrix}$ . Let  $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$  be a  $(2l + 1) \times (2l + 1)$  matrix where  $A, B, C, D$  are  $l \times l$  matrices. The matrices  $X = (X_1, X_2, \dots, X_l)$ ,  $Y = (Y_1, Y_2, \dots, Y_l)$ ,  $E = {}^T(E_1, E_2, \dots, E_l)$  and  $F = {}^T(F_1, F_2, \dots, F_l)$ . Let  $\alpha \in \mathbb{F}_q$ . Let us note the effect of multiplication by elements of one of the types from above.

$$\begin{aligned} CG1 : \quad & \begin{pmatrix} 1 & & \\ & R & \\ & & {}^T R^{-1} \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ RE & RA & RB \\ {}^T R^{-1} F & {}^T R^{-1} C & {}^T R^{-1} D \end{pmatrix} \\ & \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & & \\ & R & \\ & & {}^T R^{-1} \end{pmatrix} = \begin{pmatrix} \alpha & XR & Y {}^T R^{-1} \\ E & AR & B {}^T R^{-1} \\ F & CR & D {}^T R^{-1} \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} CG2 : \quad & \begin{pmatrix} 1 & & \\ & I & R \\ & & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E + RF & A + RC & B + RD \\ F & C & D \end{pmatrix} \\ & \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & & \\ & I & R \\ & & I \end{pmatrix} = \begin{pmatrix} \alpha & X & XR + Y \\ E & A & AR + B \\ F & C & CR + D \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} CG3 : \quad & \begin{pmatrix} 1 & & \\ & I & \\ & R & I \end{pmatrix} \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ RE + F & RA + C & RB + D \end{pmatrix} \\ & \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix} \begin{pmatrix} 1 & & \\ & I & \\ & R & I \end{pmatrix} = \begin{pmatrix} \alpha & X + YR & Y \\ E & A + BR & B \\ F & C + DR & D \end{pmatrix}. \end{aligned}$$

CG4: We only write equations that we need.

- Let the matrix  $g$  has  $C = \text{diag}(d_1, \dots, d_l)$ .

$$[(I + te_{0,-i} - 2te_{i,0} - t^2 e_{i,-i})g]_{0,i} = X_i + td_i$$

$$[g(I + te_{0,-i} - 2te_{i,0} - t^2 e_{i,-i})]_{-i,0} = F_i - 2td_i.$$

- Let the matrix  $g$  has  $A = \text{diag}(d_1, \dots, d_l)$ .

$$[(I + te_{0,i} - 2te_{-i,0} - t^2 e_{-i,i})g]_{0,i} = X_i - td_i$$

$$[g(I + te_{0,i} - 2te_{-i,0} - t^2 e_{-i,i})]_{i,0} = E_i - 2td_i.$$

6.5.1. *The Algorithm.* An overview of the algorithm is as follows:

Step 1: **Input:** matrix  $g = \begin{pmatrix} \alpha & X & Y \\ E & A & B \\ F & C & D \end{pmatrix}$  which belongs to  $O(2l + 1, q)$ ;

**Output:** matrix  $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$  of one of the following kind:

- a:  $C_1$  is a diagonal matrix  $\text{diag}(1, \dots, 1, \lambda)$  with  $\lambda \neq 0$ .

b:  $C_1$  is a diagonal matrix  $\text{diag}(1, \dots, 1, 0, \dots, 0)$  with number of 1s equal to  $m$  and  $m < l$ .

**Justification:** Using CG1 we can do row and column operations on  $C$ .

Step 2: **Input:** matrix  $g_1 = \begin{pmatrix} \alpha & X_1 & Y_1 \\ E_1 & A_1 & B_1 \\ F_1 & C_1 & D_1 \end{pmatrix}$ .

**Output:** matrix  $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$  of one of the following kind:

a:  $C_2$  is  $\text{diag}(1, 1, \dots, 1, \lambda)$  with  $\lambda \neq 0$ ,  $X_2 = 0 = F_2$  and  $A_2$  is of the form  $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & a_{22} \end{pmatrix}$  where  $A_{11}$  is skew-symmetric of size  $l-1$  and  $A_{12} = -\lambda^T A_{21}$ .

b:  $C_2$  is  $\text{diag}(1, \dots, 1, 0, \dots, 0)$  with number of 1s equal to  $m$ ;  $X_2$  and  $F_2$  have first  $m$  entries 0, and  $A_2$  is of the form  $\begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix}$  where  $A_{11}$  is an  $m \times m$  skew-symmetric.

**Justification:** Once we have  $C_1$  in diagonal form we use CG4 to change  $X_1$  and  $F_1$  in the required form. Then Lemma 6.8 makes sure that  $A_1$  has required form.

Step 3: **Input:** matrix  $g_2 = \begin{pmatrix} \alpha_2 & X_2 & Y_2 \\ E_2 & A_2 & B_2 \\ F_2 & C_2 & D_2 \end{pmatrix}$ .

**Output:**

a: matrix  $g_3 = \begin{pmatrix} \alpha_3 & 0 & Y_3 \\ E_3 & 0 & B_3 \\ 0 & C_3 & D_3 \end{pmatrix}$  where  $C_3$  is  $\text{diag}(1, 1, \dots, 1, \lambda)$ .

b: matrix  $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$  where  $C_3$  is  $\text{diag}(1, \dots, 1, 0, \dots, 0)$  with number of 1s equal to  $m$ ;  $X_3$  and  $F_3$  have first  $m$  entries 0, and  $A_3$  is of the form  $\begin{pmatrix} 0 & 0 \\ A_{21} & A_{22} \end{pmatrix}$ .

**Justification:** Observe the effect of CG2 and the Lemma 6.5 ensures the required form.

Step 4: **Input:**  $g_3 = \begin{pmatrix} \alpha_3 & X_3 & Y_3 \\ E_3 & A_3 & B_3 \\ F_3 & C_3 & D_3 \end{pmatrix}$ .

**Output:**  $g_4 = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$  with  $A_4$  diagonal matrix  $\text{diag}(1, \dots, 1, \lambda)$ .

**Justification:** In the first case, interchange rows  $i$  and  $-i$  for all  $1 \leq i \leq l$ . Now the matrix is in the form so that we can apply Lemma 6.10 and get the required result. In the second case we interchange  $i$  with  $-i$  for  $1 \leq i \leq m$ . This will make  $C_3 = 0$ . Then if needed we use CG1 on  $A_3$  to make it diagonal. The Lemma 6.9 ensures that  $A_3$  has full rank. Further we can use CG4 to make  $X_3 = 0$  and  $E_3 = 0$ . The Lemma 6.10 gives the required form.

Step 5: **Input:**  $g_4 = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & A_4 & B_4 \\ 0 & 0 & A_4^{-1} \end{pmatrix}$  with  $A_4 = \text{diag}(1, \dots, 1, \lambda)$ .

**Output:**  $g_5 = \text{diag}(\pm 1, 1, \dots, 1, \lambda, 1, \dots, 1, \lambda^{-1})$ .

**Justification:** Lemma 6.11 ensures that  $B_4$  is of a certain kind. We can use CG2 to make  $B_4 = 0$ .

Step 6: **Input:** matrix  $\text{diag}(\pm 1, 1, \dots, 1, \lambda, 1, \dots, 1, \lambda^{-1})$ .

**Output:** Identity matrix.

**Justification:** Write  $\lambda$  as  $\zeta$  times a square and use the third part of Lemma 6.7 to reduce the matrix to  $\text{diag}(1, 1, \dots, 1, \zeta, 1, \dots, 1, \zeta^{-1})$  where  $\zeta$  is a fixed non-square. Now multiplying with  $d(\zeta)$  we get the required result.

## 7. SECURITY OF THE PROPOSED MOR CRYPTOSYSTEM

The purpose of this section is to show that for a secure MOR cryptosystem over the classical Chevalley groups we have to look at automorphisms that act by conjugation, like the inner automorphisms. There are other automorphisms that also act by conjugation, like the diagonal automorphism and the graph automorphism for  $D_l$  type. Then we argue what is the hardness of our security assumptions.

Let  $\phi$  be an automorphism of one of the classical Chevalley groups  $G$ :  $\text{SL}(l+1, q)$ ,  $\text{O}(2l+1, q)$ ,  $\text{Sp}(2l, q)$ , or  $\text{O}(2l, q)$  of  $A_l, B_l, C_l$  or  $D_l$  type respectively. The automorphisms of these groups are described in Section 5. From Theorem 5.1 we know that  $\phi = c_\chi \iota \delta \gamma \theta$  where  $c_\chi$  is a central automorphism,  $\iota$  is an inner automorphism,  $\delta$  is a diagonal automorphism,  $\gamma$  is a graph automorphism and  $\theta$  is a field automorphism.

The group of central automorphisms are too small and the field automorphisms reduce to a discrete logarithm in the field  $\mathbb{F}_q$ . So there is no benefit of using these in a MOR cryptosystem. Also there are not many graph automorphisms in classical Chevalley groups other than the  $A_l$  and  $D_l$  case. In the  $D_l$  case these automorphisms act by conjugation. Recall here that, our automorphisms are presented as action on generators. It is clear [17, Section 7] that if we can recover the conjugating matrix from the action on generators, then the security is  $\mathbb{F}_{q^d}$ , if not then the security is  $\mathbb{F}_{q^{d^2}}$ .

So from these we conclude that for a secure MOR cryptosystem we must look at automorphisms that act by conjugation, like the inner automorphisms. Inner automorphisms form a normal subgroup of  $\text{Aut}(G)$  and usually constitute the bulk of automorphisms. If  $\phi$  is an inner automorphism, say  $\iota_g: x \mapsto gxg^{-1}$ , we would like to determine the conjugating element  $g$ . For  $A_l$ , the special linear group, it was done in [17]. We will follow the steps there for the present situation too. However, before we do that, let us digress briefly to observe that  $G \rightarrow \text{Inn}(G)$  given by  $g \mapsto \iota_g$  is a surjective group homomorphism. Thus if  $G$  is generated by  $g_1, g_2, \dots, g_s$  then  $\text{Inn}(G)$  is generated by  $\iota_{g_1}, \dots, \iota_{g_s}$ . Let  $\phi \in \text{Inn}(G)$ .

If we can find  $g_j, j = 1, 2, \dots, r$ , generators, such that  $\phi = \prod_{j=1}^r \iota_{g_j}$  then  $\phi = \iota_g$  where

$g = \prod_{j=1}^r g_j$ . This implies that our problem is equivalent to solving the word problem in

$\text{Inn}(G)$ . Note that solving word problem depends on how the group is represented and it is not invariant under group homomorphisms. Thus the algorithm described earlier to solve the word problem in the classical Chevalley groups does not help us in the present case.

**7.1. Reduction of security.** In this subsection, we show that for  $A_l$  and  $C_l$  case, the security of the MOR cryptosystem is the hardness of the discrete logarithm problem in  $\mathbb{F}_{q^d}$ . This is the same as saying that we can find the conjugating matrix up to a scalar multiple. We further show that the method that works for  $A_l$  and  $C_l$  does not work for  $B_l$  and  $D_l$ . Let  $\phi$  be an automorphism that works by conjugation, i.e.,  $\phi = \iota_g$  for some  $g$  and we try to determine  $g$ .

**Step 1:** The automorphism  $\phi$  is presented as action on generators  $x_r(t) = I + te_r$  except  $CG4$  in  $B_l$  type. Thus  $\phi(x_r(t)) = g(I + te_r)g^{-1} = I + tge_rg^{-1}$  where  $r \in \Phi$ . This implies that we know  $ge_rg^{-1}$  for all  $r \in \Phi$ . We first claim that we can determine  $N := gD$  where  $D$  is sparse, in fact, diagonal in the case of  $A_l$  and  $C_l$  type.

In the case of  $A_l$ , write  $g = [G_1, \dots, G_i, \dots, G_{l+1}]$ , where  $G_i$  are column vectors of  $g$ . Then  $ge_{i,j} = [G_1, \dots, G_{l+1}]e_{i,j} = [0, \dots, 0, G_i, 0, \dots, 0]$  where  $G_i$  is at the  $j^{\text{th}}$  place. Multiplying this with  $g^{-1}$  on the right, i. e., computing  $ge_{i,j}g^{-1}$  determines  $G_i$  up to a scalar multiple, say  $d_i$ . Thus, we know  $N = gD$  where  $D = \text{diag}(d_1, \dots, d_{l+1})$ .

For the  $C_l$  type we do the similar computation with the generators  $I + te_{i,-i}$  and  $I + te_{-i,i}$ . Write  $g$  in the column form as  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}]$ . Now,

- (1)  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}]e_{i,-i} = [0, \dots, 0, G_i, 0, \dots, 0]$  where  $G_i$  is at  $-i^{\text{th}}$  place. Multiplying this further with  $g^{-1}$  gives us scalar multiple of  $G_i$ , say  $d_i$ .
- (2)  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}]e_{-i,i} = [0, \dots, 0, G_{-i}, 0, \dots, 0]$  where  $G_{-i}$  is at  $i^{\text{th}}$  place. Multiplying this with  $g^{-1}$  gives us scalar multiple of  $G_{-i}$ , say  $d_{-i}$ .

Thus we get  $N = gD$  where  $D$  is a diagonal matrix  $\text{diag}(d_1, \dots, d_l, d_{-1}, \dots, d_{-l})$ .

For  $D_l$  type, write  $g = [G_1, \dots, G_l, G_{-1}, \dots, G_{-l}]$ . Now computing  $ge_rg^{-1}$  gives the following equations:

- (1)  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}](e_{i,j} - e_{-j,-i})g^{-1} = [0, \dots, 0, G_i, 0, \dots, 0, G_{-j}, 0, \dots]g^{-1}$  where  $G_i$  is at  $j^{\text{th}}$  place and  $G_{-j}$  is at  $-i^{\text{th}}$  place. This gives us linear combination of the columns  $G_i$  and  $G_{-j}$ .
- (2)  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}](e_{i,-j} - e_{j,-i})g^{-1} = [0, \dots, 0, G_i, 0, \dots, 0, G_j, 0, \dots]g^{-1}$  where  $G_i$  is at  $-j^{\text{th}}$  place and  $G_j$  is at  $-i^{\text{th}}$  place. This will give us linear combination of the columns  $G_i$  and  $G_j$ .
- (3)  $[G_1, \dots, G_l, G_{-1}, \dots, G_{-l}](e_{-i,j} - e_{j,i})g^{-1} = [0, \dots, 0, G_{-i}, 0, \dots, 0, G_{-j}, 0, \dots]g^{-1}$  where  $G_{-i}$  is at  $j^{\text{th}}$  place and  $G_{-j}$  is at  $i^{\text{th}}$  place. This will give us linear combination of the columns  $G_{-i}$  and  $G_{-j}$ .

Thus we get  $N = gD$  where  $D$  is of the form  $\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$  with  $W$  a diagonal matrix,  $Y$  anti-diagonal,  $X$  has first column nonzero and  $Z$  has the last column nonzero. This is not a diagonal matrix. One can do a similar computation for  $B_l$  type.

**Step 2:** Now we compute  $N^{-1}\phi(x_r(t))N = D^{-1}g^{-1}(gx_r(t)g^{-1})gD = I + D^{-1}e_rD$  which is equivalent to computing  $D^{-1}e_rD$  for  $r \in \Phi$ .

In the case of  $A_l$  we have  $D$  diagonal. Thus by computing  $D^{-1}e_{i,j}D$  we determine  $d_i^{-1}d_j$  for  $i \neq j$  and form a matrix  $\text{diag}(1, d_2^{-1}d_1, \dots, d_l^{-1}d_1)$  and multiply this to  $N$  we get  $d_1g$ . Hence we can determine  $g$  up to a scalar matrix.

In the  $C_l$  case we can do similar computation as  $D$  is diagonal. First compute  $D^{-1}(e_{i,j} - e_{-j,-i})D$  to get  $d_i^{-1}d_j$  and  $d_{-i}^{-1}d_{-j}$  for  $i \neq j$ . Now compute  $D^{-1}e_{i,-i}D, D^{-1}e_{-i,i}D$  to get  $d_id_{-i}^{-1}, d_{-i}d_i^{-1}$ . We form a matrix

$$\text{diag}(1, d_2^{-1}d_1, \dots, d_l^{-1}d_1, d_{-1}^{-1}d_{-2}, d_{-2}^{-1}d_{-2}, d_2^{-1}d_1, \dots, d_{-l}^{-1}d_{-1}, d_{-1}^{-1}d_1)$$



and multiply it to  $N = gD$  to get  $d_1g$ . Thus we can determine  $g$  up to a scalar multiple and then the attack follows [17, Section 7.1.1].

However in the case of  $B_l$  and  $D_l$  the matrix  $D$  is not a diagonal matrix and the above method to determine  $g$  does not work.

## 8. CONCLUSION

This section is similar to [17, Section 8]. An useful public-key cryptosystem is a delicate dance between speed and the security. So one must talk about speed along with security. As we said in the introduction, this study was to find the embedding degree for the symplectic and orthogonal groups over finite fields of odd characteristic. So we will be somewhat brief with implementation details.

The implementation that we have in mind uses the row-column operations. Let  $\langle g_1, g_2, \dots, g_s \rangle$  be a set of generators for the orthogonal or symplectic group as described before. As is the custom with a MOR cryptosystem, the automorphisms  $\phi$  and  $\phi^m$  are presented as action on generators, i.e., we have  $\phi(g_i)$  and  $\phi^m(g_i)$  as matrices for  $i = 1, 2, \dots, s$ .

To encrypt a message in this MOR cryptosystem, we compute  $\phi^r$ . We do that by *square-and-multiply* algorithm. For this implementation, squaring and multiplying is almost the same. So we will refer to both squaring and multiplication as multiplication. Note that multiplication is composing of automorphisms.

The implementation that we describe in this paper, can work in parallel. Each instance computes  $\pi^r(g_i)$  for  $i = 1, 2, \dots, s$ . First thing that we do is write the matrix of  $\phi(g_i)$  as a word in generators. So essentially the map  $\phi$  becomes a map  $g_i \mapsto w_i$  where  $w_i$  is a word in generators of some fixed length. Then multiplication becomes essentially a replacement, replace all instances of  $g_i$  by  $w_i$ . This can be done very fast. However, the length of the replaced word can become very large. The obvious question is, how soon are we going to write this word as a matrix. This is a difficult question to answer at this stage and depends on available computational resources.

Once we decide how often we change back to matrices, how are we going to change back to matrices? There can be a fairly easy *time-memory* trade-offs. Write all words up to a fixed length and the corresponding matrix as a pre-computed table and use this table to compute the matrices. Once we have matrices, we can multiply them together to generate the final output. If writing all words is impossible, due to resource constraint, write some of it in a table. There are also many obvious relations among the generators of these groups. One can just store and use them. The best strategy for an efficient implementation is yet to be determined. It is clear now that there are many interesting and novel choices.

The benefits of this MOR cryptosystem are:

- : This can be implemented in parallel easily.
- : This implementation doesn't depend on the size of the characteristic of the field. This is an important property in light of Joux's recent improvement of the index-calculus attacks [2].

There is one issue with this MOR cryptosystem, the key-size is large. For parameters and complexity analysis of this cryptosystem, we refer to [17, Section 8].

**8.1. Further Research.** We conclude this paper with two open directions for further research.

- : What is the most efficient strategy to implement the MOR cryptosystem on Orthogonal and Symplectic groups that we described earlier?
- : What is the security for the twisted groups?

## REFERENCES

1. R. Balasubramanian and N. Koblitz, *The improbability than an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology **11** (1998), no. 2, 141–145.
2. Razvan Barbulescu, Plerrick Gaudry, Antoine Joux, and Emmanuel Thome, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, Eurocrypt2014, 2014, pp. 1–16.
3. E. I. Bunina, *Automorphisms of chevalley groups of type B over local rings with  $1/2$* , Fundam. Prikl. Mat. **15** (2009), no. 7, 3–46.
4. ———, *Automorphisms of chevalley groups of types  $A_l$ ,  $D_l$ , and  $E_l$  over local rings with  $1/2$* , Fundam. Prikl. Mat. **15** (2009), no. 2, 35–59.
5. Roger Carter, *Simple groups of Lie type*, Pure and Applied Mathematics, vol. 28, John Wiley & Sons, 1972.
6. C. Chevalley, *Sur certains groupes simples*, Tohoku Math. J. **7** (1955), no. 2, 14–66.
7. Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Mathematics of computation **73** (2003), no. 247, 1477–1498.
8. Jean Dieudonne, *On the automorphisms of the classical groups. with a supplement by Loo-Keng Hua*, Memoirs of the American Mathematical Society, 1951.
9. Larry C. Grove, *Classical groups and geometric algebra*, vol. 39, American Mathematical Society, Graduate Studies in Mathematics, 2002.
10. R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky, *Presentations of finite simple groups: profinite and cohomological approaches*, Groups Geom. Dyn. **1** (2007), no. 4, 469–523.
11. ———, *Presentations of finite simple groups: a quantitative approach*, J. Amer. Math. Soc. **21** (2008), no. 3, 711–774.
12. ———, *Presentations of finite simple groups: a computational approach*, J. Eur. Math. Soc. **13** (2011), no. 2, 391–458.
13. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An introduction to mathematical cryptography*, Springer, 2008.
14. Antoine Joux, *A new index calculus algorithm with complexity  $L(1/4 + o(1))$  in small characteristic*, SAC2013, 2013, pp. 355–379.
15. Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions (English summary) with a preface in French by J. Tits*, vol. 44, American Mathematical Society Colloquium Publications, 1998.
16. C. R. Leedham-Green and E. A. O’Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881.
17. Ayan Mahalanobis, *A simple generalization of the ElGamal cryptosystem to non-abelian groups II*, Communications in Algebra **40** (2012), no. 9, 3583–3596.
18. ———, *The MOR cryptosystem and finite p-groups*, Contemporary Mathematics, American Mathematical Society, 2014, to appear.
19. Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park, *New public key cryptosystem using finite non-abelian groups*, Crypto 2001 (J. Kilian, ed.), LNCS, vol. 2139, Springer-Verlag, 2001, pp. 470–485.
20. G. B. Seligman, *Modular Lie algebras*, Springer-Verlag, 1967.
21. Joseph Silverman and Joe Suzuki, *Elliptic curve discrete logarithms and the index calculus*, Asiacrypt’98 (K. Ohra and D. Pei, eds.), LNCS, vol. 1514, 1998, pp. 110–125.
22. Robert Steinberg, *Automorphisms of finite linear groups*, Canadian Journal of Mathematics **12** (1960), 606–615.
23. ———, *Lectures on Chevalley groups. notes prepared by John Faulkner and Robert Wilson*, Yale University, 1968.

24. Nikolai Vavilov, *Structure of chevalley groups over commutative rings*, Nonassociative algebras and related topics (Hiroshima, 1990), World Sci. Publ., River Edge, NJ, 1991, pp. 219–335.